Statement of the
Honorable William A. Reinsch
Under Secretary for Export Administration
Department of Commerce

Before

Subcommittee on Communications
Committee on Commerce, Science and Transportation
U.S. Senate

March 8, 2000

Mr. Chairman, I welcome this opportunity to appear before you to discuss the Federal government's efforts to protect the nation's critical infrastructures.

Interdependent computer networks are an integral part of doing business in the Information Age. America is increasingly dependent upon computer networks for essential services, such as banking and finance, emergency services, delivery of water, electricity and gas, transportation, and voice and data communications. New ways of doing business in the 21st century are rapidly evolving. Business is increasingly relying on E-commerce for its commercial transactions as well as for its critical operations. At the same time, recent hacking attempts at some of the most popular commercial Web sites underscore that America's information infrastructure is an attractive target for deliberate attack or sabotage. These attacks can originate from a host of sources, such as terrorists, criminals, hostile nations, or the equivalent of car thief “joyriders.” Regardless of the source, however, the potential for cyber damage to our national security and economy is evident.

Protecting our critical infrastructures requires that we draw on various assets of the government. When specific incidents or cyber events occur, the government needs a capacity to issue warnings, investigate the incident, and develop a case to punish the offenders. The National Information Protection Center at the FBI is organized to deal with such events as they occur.

Over the long term, the government also has a duty to be proactive to ensure that our computer systems are protected from attack. Critical infrastructure protection involves assets of both the government and the private sector. A number of agencies have responsibilities with respect to government computer systems. The Department of Defense is well on its way to securing its critical systems, and the Office of Management and Budget (OMB) and the National Institute of Standards and Technology at the Department of Commerce (NIST) have responsibility for information resources management of computer systems in Federal agencies.

I want to make clear that the Federal government's responsibility in this area with respect to the commission of crimes is only part of the equation. The infrastructures at risk are owned and operated by the private sector. The use of information technology is so embedded in the core operations and customer service delivery systems of industry that inevitably, it will be they who must work together to take the steps necessary to protect themselves. We can help. The first major step is the elevation of awareness across industry of the “business case for action” for leaders within industry. They have a commercial interest in maintaining a secure business environment that assures public confidence in their institutions. We can also help identify problems, good practices in management policies and strategies, and publicize them, encourage planning, promote research and development, convene meetings. In short, we can act as a catalyst for industry to mobilize. That is precisely the role the Commerce Department is playing in several ways.

First, the National Telecommunications and Information Administration (NTIA) is lead agency for the communications and information sector. In February, 199, NTIA created a Private Sector Coordinator Consortium. This role is filled by representatives from the Information Technology Association of America (ITAA), the Telecommunications Industry Association (TIA), and the U.S. Telecom Association (USTA). Among their initiatives, the consortium has been raising awareness among industry through the exchange of information on threats and vulnerabilities, conducting information security surveys acrsoss sectors, and developing and asessing CIP-related standards and best practices.

Another active area is the development of the Partnership for Critical Infrastructure Security. The Partnership is a collaborative effort between industry and government. This undertaking brings representatives of the infrastructure sectors together in a dialogue with each other and with other stakeholders, including the risk management and investment communities, mainstream businesses, and state and local governments.

The Partnership complements the work of the federal lead agencies responsible for working directly with the industry sectors in developing their critical infrastructure plans, including NTIA’s work with the communications and information technology industries. It also complements the NIPC’s focus on cyber-terrorism by encouraging industry to collaborate on information security issues.

Secretary Daley, Assistant Secretary for Communications and Information Gregory Rohde, and I met with senior members of over 80 Partnership companies in December in New York. We met again last month in Washington, D.C., with over 220 senior members of more than 120 Partnership companies to encourage business leaders to adopt information security as an integral business practice. The Partnership agreed to address such important issues as, cross-sector vulnerability assessments, information sharing, and R&D requirements.

The Commerce Department’s Critical Infrastructure Assurance Office (CIAO) also is assisting Federal agencies in conducting analyses of their own dependencies on critical infrastructures. CIAO has just finished an ambitious pilot program that identifies the critical assets of the Commerce Department and maps out dependencies on governmental and private sector infrastructures. This program will provide important input to managers and security officials as they seek to assure their critical assets against cyber attacks.

The Commerce Department, through the CIAO, coordinated the development of the *National Plan for Information Systems Protection*. President Clinton announced the release of Version 1.0 of the Plan on January 7.

It represents the first attempt by any national government to design a way to protect those infrastructures essential to the delivery of electric power, oil and gas, communications, transportation services, banking and financial services, and vital human services. Increasingly, these infrastructures are being operated and controlled through the use of computers and computer networks.

The current version of the Plan focuses mainly on the domestic efforts being undertaken by the Federal government to protect the Nation's critical cyber-based infrastructures. Later versions will focus on the efforts of the infrastructure owners and operators, as well as the risk management and broader business community. Subsequent versions will also reflect to a greater degree the interests and concerns expressed by Congress and the general public based on their feedback. That is why the Plan is designated *Version 1.0* and subtitled *An Invitation to a Dialogue* -- to indicate that it is still a work in progress and that a broader range of perspectives must be taken into account if the Plan is truly to be "national" in scope and treatment.

II. The Plan: Overview and Highlights

President Clinton directed the development of this Plan to chart the way toward the attainment of a national capability to defend our critical infrastructures by the end of 2003. To meet this ambitious goal, the Plan establishes 10 programs for achieving three broad objectives. They are:

Objective 1: Prepare and Prevent: Undertake those steps necessary to minimize the possibility of a significant and successful attack on our critical information networks, and build an infrastructure that remains effective in the face of such attacks.

<u>Program 1</u> calls for the government and the private sector to identify significant assets, interdependencies, and vulnerabilities of critical information networks from attack, and to develop and implement realistic programs to remedy the vulnerabilities, while continuously updating assessment and remediation efforts.

Objective 2: Detect and Respond: Develop the means required to identify and assess attacks in a timely way, contain such attacks, recover quickly from them, and reconstitute those systems affected.

<u>Program 2</u> will install multi-layered protection on sensitive computer systems, including advanced fire walls, intrusion detection monitors, anomalous behavior identifiers, enterprise-wide management systems, and malicious code scanners. To protect critical Federal systems, computer security operations centers will receive warnings from these detection devices, as well as Computer Emergency Response

Teams (CERTs) and other means, in order to analyze the attacks, and assist sites in defeating attacks.

Program 3 will develop robust intelligence and law enforcement capabilities to protect critical information systems, consistent with the law. It will assist, transform, and strengthen U.S. law enforcement and intelligence agencies to be able to deal with a new kind of threat and a new kind of criminal -- one that acts against computer networks.

Program 4 calls for a more effective nationwide system to share attack warnings and information in a timely manner. This includes improving information sharing within the Federal government and encouraging private industry, as well as, state and local governments, to create Information Sharing and Analysis Centers (ISACs), which would share information among corporations and state and local governments, and could receive warning information from the Federal government. Program 4 additionally calls for removal of existing legal barriers to information sharing.

Program 5 will create capabilities for response, reconstitution, and recovery to limit an attack while it is underway and to build into corporate and agency continuity and recovery plans the ability to deal with information attacks. The goal for government and the recommendation for industry is that every critical information system have a recovery plan in place that includes provisions for rapidly employing additional defensive measures (e.g., more stringent firewall instructions), cutting off or shutting down parts of the network under certain predetermined circumstances (through enterprise-wide management systems), shifting minimal essential operations to “clean” systems, and to quickly reconstitute affected systems.

Objective 3: Build Strong Foundations: Take all actions necessary to create and support the Nation’s commitment to Prepare and Prevent and to Detect and Respond to attacks on our critical information networks.

Program 6 will systematically establish research requirements and priorities needed to implement the Plan, ensure funding, and create a system to ensure that our information security technology stays abreast with changes in the threat environment.

Program 7 will survey the numbers of people and the skills required for information security specialists within the Federal government and the private sector, and takes action to train current Federal IT workers and recruit and educate additional personnel to meet shortfalls.

Program 8 will explain publicly the need to act now, before a catastrophic event, to improve our ability to defend against deliberate cyber-based attacks.

Program 9 will develop the legislative framework necessary to support initiatives proposed in other programs. This action requires intense cooperation within the Federal government, including Congress, and between the government and private industry.

Program 10 builds mechanisms to highlight and address privacy issues in the development of each and every program. Infrastructure assurance goals must be accomplished in a manner that maintains, and even strengthens, American's privacy and civil liberties. The Plan outlines nine specific solutions, which include consulting with various communities; focusing on and highlighting the impact of programs on personal information; committing to fair information practices and other solutions developed by various working groups in multiple industries; and working closely with Congress to ensure that each program meets standards established in existing Congressional protections.

With respect to funding, President Clinton has proposed increases for critical infrastructure protection substantially over the past three years, including a 15% increase in his FY 2001 budget to $2.01 billion. He has also developed and funded new initiatives to defend the nation's systems from cyber attack:

C Establishing a permanent Expert Review Team (ERT) at NIST that will help agencies conduct vulnerability analyses and develop critical infrastructure protection plans. ($5 million).

C Working to recruit, train, and retrain Federal IT Experts. We have developed and provided FY2001 funding for a Federal Cyber Services Training and Education initiative led by OPM and NSF which calls for two programs: the first is an ROTC-like program where we pay for IT education (B.S. or M.S.) in exchange for federal service; and the second is a program to establish competencies and certify our existing IT workforce. ($25 million).

C Funding seven Public Key Infrastructure model pilot programs in FY 2001 at different Federal agencies. ($7 million).

C Designing a Federal Intrusion Detection Network (FIDNET) to protect vital systems in Federal civilian agencies, and in ensuring the rapid implementation of system "Apaches" for known software defects. FIDNET will operate in full compliance with all existing privacy laws. ($10 million).

C Developing Federal R&D Efforts. R&D investments in computer security will grow by 31% in the FY 2001 budget. ($606 million).

C Establishing an Institute for Information Infrastructure Protection. The Institute would identify and address serious R&D gaps that neither the private sector nor the government's national security community would otherwise address, but that are necessary to ensure the robust, reliable operation of the national information infrastructure. The President's FY2001 budget provides funding of $50 million for the Institute. Funding would be provided through the Commerce Department's National Institute of Standards and Technology (NIST) to this organization. The Institute was first proposed by the scientists and corporate officials who served on the President's Committee of Advisors on Science and Technology, and supported by leading corporate Chief Technology officers. ($50 million).

C National Infrastructure Assurance Council (NIAC). The President signed an Executive order creating this Advisory Council last year. Its members are now being recruited from senior ranks of the critical infrastructure industries, including the information technology, and state and local governments.

In addition, the President announced a number of new initiatives designed to support efforts for enhancing computer security, including a $9 million FY 2000 budget supplemental to jump-start key elements of next year’s budget.

In early February, Secretary Daley met with the President and 25 senior executives concerned about the recent disruptions to the Internet. This meeting reinforced the need for further cooperation between government and industry to help the private sector develop its action agenda for cyber security. The incidents of early February are not cause for pushing the panic button, but they are a wake up call for action. As the President said, “I think there is a way that we can clearly promote security.” The President has submitted a budget proposal that funds a number of initiatives that address critical information systems protection. If we are to reap the benefits of the Information Age, we need to take action to maintain public confidence in a secure business environment that ensures both our national security and the growth of our economy.